REMARKS/ARGUMENTS

Claim Amendments

The Applicant has amended claims 1, 7, 11, 13, 16-17 and 20. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-13 and 15-25 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

Applicant Remarks and response

The Applicant notes that claims 3-4 and 16-17 were not commented on by the Examiner in the last Office Action. The Applicant has provided amendments to the claims to disclose the term "multicast in the bodies of independent claims that were lacking the terminology. Support for this amendment is found on page 9, lines 2-5.

The Fox reference discloses comparing hash values to determine if the participant actually created the encrypted hash to prove the origin of the participant. The cited reference in Fox does disclose the comparison of hash values but, the Applicant claims the use of the private key along with a cryptographic hashing of a random number and a time-stamp.

Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1, 3-4, 13, and 16-17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nikander (GB 2367986 A) in view of Fox, et al. (US Patent 5,790,677 and Fox hereinafter). The Applicant respectfully traverses the rejection of these claims.

The present invention discloses an authentication scheme for handling individual members of a multicast group, upon leaving and joining the group, so that the members can access the multicast content when they join and be prevented from accessing the content when they leave the group. The scheme uses the member's public-private key and IPv6 address, transmitted to a group controller by the member, to confirm that the public key is associated with the member's IPv6 address and the member is at the IPv6 address. In order to confirm that the member is in actual possession of the address and the public-private key, the group controller sends a random number, a time stamp and the member cryptographically hashes these using the private key to generate a digital signature verifying the member's public-private key. The terminal applies the private key to the certificate and the signature is returned to the controller (page 11, lines 15-26).

The object of the Nikander reference is to provide a means for proving ownership of an IP address. Nikander discloses application of a coding function to components received from a host and comparing the results against the interface identifier part of the IP address. If the results match the interface identifier, the host is then assumed to be authorized to use the IP address and if no match, the host is not authorized.

The Nikander reference fails to disclose the use of the private key of the member in a digital signature to further verify that the candidate member (actually, terminal) owns the public-private key pair to which the public key belongs and that the candidate member terminal owns or is at the source IP address.

The Applicant respectfully submits that a registration message including "...a digital signature using the candidate member's private key... is not disclosed in the Nikander or Fox references. Though the use of IPv6 addressing is disclosed in the Nikander reference, the Fox reference does not use IPv6. Fox though, is cited for teaching use of the candidate member's private key, but Fox actually does not use the private key. The Examiner comments that the features are well known in the art and states that the Nikander reference when modified by the Fox reference discloses use of the private portion of the key (page 5, lines 9-10 of the Office Action). However, a close reading of the Fox reference discloses use of a public key and digital signature for registration. Support for this is found in Fox where the registration packet includes "...public cryptography keys unique to the participant and a digital signature of the participant" (col 8, lines 39-42). Nowhere in the cited portion of Fox is the use of a private key mentioned. Fox thus does not disclose the use of a private key as claimed in claim 1.

The Applicant respectfully submits that the Fox reference also does not disclose multicast which is defined in the Applicant's specification on page 1, lines 21-27 defines "multicast":

> *"An IP technology that allows for streams of data to be sent efficiently from one to many destinations. Instead of setting up separate unicast sessions for each destination, multicast will replicate packets at router hops where the path to different multicast group members diverges. This allows a source to send a single copy of a stream of data, while reaching any number of possible receivers."*

As the Fox reference fails to disclose Multicast there is no invitation to join a multicast group. The referenced portion of Fox; "[A]n application tailored to the particular commerce environment <u>can</u> be distributed to the participants to assist them in <u>gathering and submitting the information</u> required by the certified trusted authority" does not appear to be an invitation; more of a registration.

The Applicant respectfully submits that the limitations recited above that are missing from the Nikander reference and the Fox reference cause the obviousness rejection to fail. That being the case the Applicant respectfully requests the allowance of independent claims 1 and 13. The Applicant determined that the Examiner does not appear to have actually rejected, or allowed, the limitations of claims 3-4 and 16-17. However, the Applicant respectfully submits that since these claims depend from claims 1 and 13 and contain the limitations recited in claims 1 and 13, then they to are allowbable. Therefore, the allowance of claims 1, 3-4, 13, and 16-17 is respectfully requested.

Claims 2, 5-6, 15, and 18-19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nikander in view of Fox as applied to claims 1, 13 and 17 above, and further in view of Caronni et al (US Patent 6,049,878 and Caronni hereinafter). The Applicant respectfully traverses the rejection these claims.

As noted above, Nikander and Fox do not disclose at least the limitation of using the member's private key to generate a digital signature. The Caronni reference lacks these same limitations and the Applicant respectfully submits that claims 2, 5-6, 15 and 18-19 are thus allowable over Nikander, Fox and Caronni. Therefore, the allowance of these claims is respectfully requested.

Claims 7-9, 20-22 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wesley et al (US Patent 6,275,859 B1 and Wesley hereinafter) in view of Caronni and Fruehauf et al (US Patent 7,149,308 B1 and Fruehauf hereinafter). The Applicant respectfully traverses the rejection of these claims.

Claims 7 and 20 include limitations not found or taught in either the Wesley Caronni or Fruehauf references or any combination of the three. In the present application, a digital signature is generated by applying a cryptographic algorithm and the user's (terminal's) private key to the contents of a certificate. And, then a proof-of-possession procedure based on the private key is used to verify ownership of the certificate. Verifying ownership through the use of the user/terminal's ***private*** key (instead of the user's public key) ensures that the user or terminal that is submitting the private key has not stolen the certificate.

The Wesley reference is cited as disclosing this limitation (Wesley at col 3, lines 6-9 and col 4 lines 19-22). The Applicant respectfully disagrees with the Examiner's interpretation of the cited portions of Wesley; "[S]ubsequently... the nodes exchange their participation certificates to prove their identities and their authorization to participate" and "...[e]ach participation certificate 16 includes the public key half of a public/private key pair uniquely associated with the node 10 receiving the certificate...". Wesley discloses the exchange of certificates but neither Wesley, Caronni, nor Fruehauf disclose the use of a proof of possession procedure based on the private key as claimed by the Applicant in claims 7 and 20.

The Applicant respectfully submits that claims 7 and 20 are patentable over the Wesley, Caronni and Fruehauf references, as are the respective dependent claims 8-9, 21-22 and 25. The allowance of claims 7-9, 20-22 and 25 are respectfully requested.

Claims 10 and 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wesley in view of Caronni and Fruehauf as applied to claims 7 and 20 above, and further in view of Nikander. The Applicant respectfully traverses the rejection of these claims.

The Applicant previously noted that Wesley and Caronni fail to provide limitations that are not disclosed by Nikander. The Applicant respectfully submits that the Nikander reference does not disclose the user sending a response to the control node containing a signature generated by applying the <u>private</u> key to the random number. Nikander discusses the use of a public key portion of the public/private key and the Applicant claims the use of the private key. Fruehauf also fails to disclose these limitations. Since these four references fail to provide all the limitations claimed in the independent claims from which claims 10 and 23 depend, the Applicant respectfully requests the allowance of claims 10 and 23.

Claims 11-12 and 24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wesley in view of Caronni and Fruehauf as applied to claims 7 and 20 above, and further in view of Chow et al (US 2003/0053434 A1 and Chow hereinafter). The Applicant respectfully traverses the rejection of these claims

The Applicant previously noted that Wesley and Caronni fail to provide limitations that are not disclosed by Nikander. Fruehauf and Chow also fail to disclose these limitations. Since these five references fail to provide all the limitations claimed in the independent claims from which claims 10 and 23 depend, the Applicant respectfully requests the allowance of claims 10 and 23.

.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

Sidney L Weatherford

By Sidney L. Weatherford
Registration No. 45,602

Date: April 30, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-8656
sidney.weatherford@ericsson.com